E-Safety & Mobile Phones

Contents

1 Policy statement 3
2 E-Safety Incident Process 5
3 E-Safety Complaints 6
4 Mobile Phones 6
5 Email 8
6 Publishing of Pupil Images 9
7 Social Networking Access 9
8 E-Safety for Boarders 10
9 Data Protection 11
10 Sites for reference and e-Safety Guidance 11
11 Relevant Legislation 11
12 Acceptable Use Policies 12
12.1 Acceptable Use policy, Reception, Year 1 & Year 2 13
12.2 Acceptable Use Policy, Years 3-6 12
12.3 Acceptable Use Policy for Prep School Pupils 14
12.4 Acceptable Use Policy for Senior School pupils 20
Equipment / Hardware 20
iPad care, insurance and charges 21
Privacy, Data & Security 21
Academic integrity, Plagiarism and Artificial Intelligence use 21
Online behavior and communication 22
Monitor and Safeguarding 22
Breach of this policy 22
Parental Agreement 22
12.5 Acceptable Use Policy for staff 23
12.6 EMBLEY Prep School Mobile Phone Policy for Years 3 to 6 29
13 Document Information 30

1 Policy statement

1.1 E-Safety encompasses not only Internet technologies but also electronic communications such as mobile devices and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

1.2 Most Internet use in school is safe, purposeful, and beneficial to learners. However, there is always an element of risk: even an innocent search can occasionally produce links to adult content or violent imagery. With fast website access, inappropriate material can appear almost instantly, and children may inadvertently follow a series of links that lead to undesirable content.

To mitigate these risks, Embley uses Securly web filtering on all school-owned devices. This powerful safeguarding tool ensures safe internet access both on and offsite by blocking access to inappropriate websites and content. Additionally, Securly proactively monitors activity and sends alerts to key safeguarding staff if concerning behaviour or searches are detected, helping us to respond quickly and appropriately.

1.3 Curriculum Internet use produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily. Curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment in order to enrich and extend learning activities.

1.4 All staff must read and sign all 'Acceptable Use' documentation. Whenever the policy changes significantly, a new agreement will be required.

1.5 This policy applies to all members of our school community, including boarders and those in our EYFS setting.

1.6 Embley is fully committed to ensuring that the application of this E-Safety policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.

1.7 Embley seeks to implement this policy through adherence to the procedures set out in the rest of this document.

1.8 This document is available to all interested parties on our website and on request from the Senior or Prep School offices and should be read in conjunction with the following documents:

Acceptable use of ICT and digital resources
Cyber Bullying
Bullying
PSHE
Anti Bullying
Child Protection (Safeguarding)

1.9 It is important that all staff feel confident to use the Internet in teaching. The School E-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. Staff must understand that the Internet misuse rules for UCST employees are quite specific. Instances of misuse resulting in dismissal have occurred. If a member of staff is concerned about any aspect of their Internet use in school, they should discuss this with their line manager to avoid any possible misunderstanding.

1.10 Internet use is widespread and all staff including administration, governors and volunteers within the school should be included in appropriate awareness raising and training. The induction of new staff should include guidelines on appropriate use.

1.11 All staff will have access to the Embley E-Safety Policy via Staff Handbook and will have its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the SLT and have clear procedures for reporting issues.
- Staff development in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

1.12 The school allocates Internet access for staff and pupils on the basis of educational need. As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation.

1.13 EMBLEY has a disclaimer as follows:

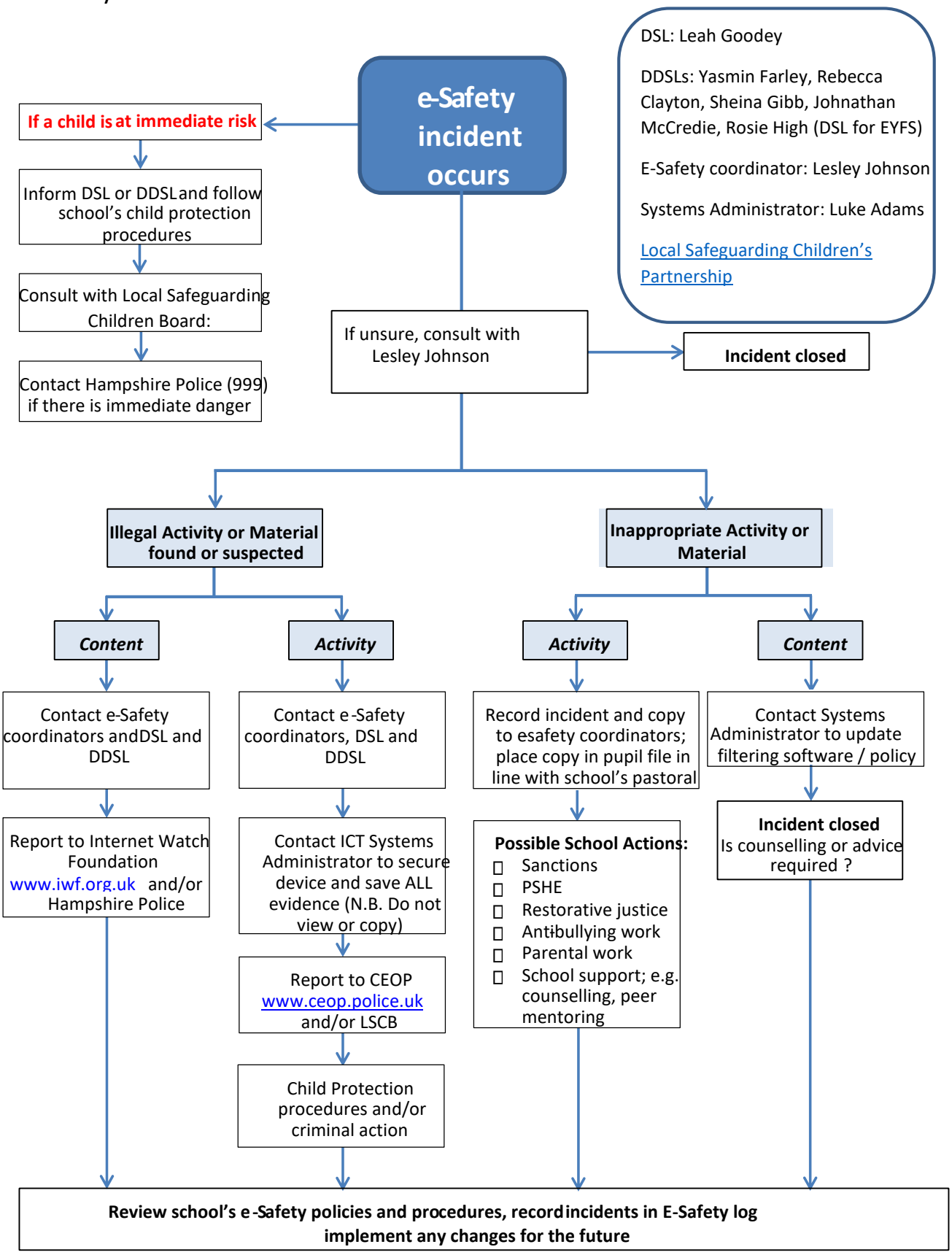
> *'In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor UCST can accept liability for the material accessed, or any consequences of Internet access.'*

1.14 The school will maintain a current record of all staff and pupils who are granted Internet access. All staff, pupils and parents must read and sign the Acceptable use of ICT and digital resources documentation before using any school ICT resource.

1.15 At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

The Governing Body, Senior Leadership Team, Designated Safeguarding Lead and IT Team will review filtering and monitoring arrangements annually and whenever significant safeguarding or technological changes occur. The school will maintain clear roles and responsibilities for the management and oversight of filtering and monitoring systems.

2 E-Safety Incident Process



3 E-Safety Complaints

3.1 Prompt action will be required if a complaint is made regarding material accessed on the Internet, either incidentally or otherwise, or in the event of an accusation of cyber-bullying, etc. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

3.2 A minor transgression of the rules may be dealt with by the teacher. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school's DSL or DDSLs.

3.3 The following overall principles apply:

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headmaster.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Procedures will be followed according to the Child Protection (Safeguarding) Policy.
- Sanctions within the school Behaviour Policy include: – interview/counselling by Head of Year or class teacher in the Prep School; – informing parents or carers; – removal of Internet or computer access for a period.

4 Mobile Phones

4.1 Embley actively discourages mobile phones being brought to school. Mobile phones are not needed by pupils whilst they are on-site, therefore we ask parents not to allow their child/children to bring a mobile phone to school. Parents can now track Embley minibuses, which will allow them to monitor their child's journey to and from school.

In accordance with Department for Education statutory guidance, Embley operates as a mobile phone-free environment during the school day. For the purpose of this policy, "mobile phones" includes smart phones, smart watches, internet-enabled communication devices and other smart technology capable of sending messages, receiving notifications, accessing the internet, taking photographs, recording audio or video, or making calls.

Smart watches and other wearable communication devices are subject to the same restrictions as mobile phones. Pupils may not use such devices to communicate, record, photograph, access the internet or receive notifications during the school day unless expressly authorised for medical reasons.

Prep School

4.2 Pupils at Embley Prep School are not allowed to have or use mobile phones at any point during the school day. Parents are reminded that in cases of emergency, the Prep School office remains the main point of contact.

4.3 Any pupil who brings a mobile phone into school must hand it into the Prep School office at the beginning of the school day and collect it at the end of the school day. The phone must be clearly named.

Senior School - Years 7-11

4.4 If a pupil brings a mobile phone to school with the permission of their parent, it should not be visible anywhere on-site from when they arrive to when they leave and must be locked away in the pupil's locker. These restrictions apply unless a pupil has been given special permission to carry or use their mobile phone for medical reasons, (such as to manage insulin levels for diabetes) usually by their Head of Year or Matron.

4.5 Any pupil seen with their mobile phone or headphones out around the campus will have:

1st offence: phone confiscated, email home and a Head of Year lunchtime detention
2nd offence: phone confiscated, email home and a Friday Senior Leadership Team detention
3rd offence: phone confiscated, phone call home and a Saturday Headmaster's detention

4.6 If a pupil needs to make a phone call home, they can use the phone in the Senior School Office. If there is a particular need for privacy then they should talk to their Head of Year and use the phone in their office as necessary.

4.7 If a parent/guardian needs to contact a pupil urgently while they are on campus, they should call Reception (01794 512206) and a message will be relayed to them.

4.8 Our expectation is that pupils do not take phones (or any other personal devices) on school trips.

Residential School Trips
4.8.1 If a pupil does bring a mobile phone on a school trip there will be times, as directed by staff, such as during activities, mealtimes or overnight when they will be required to hand it in to a member of staff. The expectation is that any mobile phones taken on a residential trip will have parental controls activated. The recommended time restrictions are from 9pm to 7am (local time).

Day trips
4.8.2 When travelling to and from mid-week sports fixtures or training, or on a one-day school trip, our expectation is that pupils do not take phones with them but leave them at school in their lockers. If a pupil is seen using their phone, they will receive a sanction in line with point 4.3. Where a school trip runs outside of normal school hours and due to the possibility of return times changing, pupils who bring a mobile phone on a trip must keep it out of sight for the duration of the trip and it can only be used when directed by a member of staff.

Saturday fixtures
4.8.3 By the changeable nature of Saturday fixtures, while phones are discouraged, if a pupil brings a mobile phone, it must not be visible for the duration and only used under the direction of a member of staff.

Sixth Form – Years 12 & 13
4.9 Sixth Form students may bring their mobile phone to school, though it is expected that they are turned to silent and only used in the Sixth Form common areas. Mobile phones are not to be visible around campus. Sixth Form students may take their phones on school trips.

Boarders
4.10 Parents of boarders are expected to enable age-appropriate parental controls on their child's mobile phone, taking into consideration such things as the timings of the school day, Prep and bedtimes. Below are links to useful information and instructions for parental controls for the most common mobile phone companies: Apple Samsung Google

4.11 Boarders are not permitted to use their phones during Prep, evening activities or meal times. During Prep, boarders in Years 7-10 hand their phones in to the member of staff on Prep duty.

Boarders in Years 7-9 hand in all electronic devices (including phones, school iPads and any personal laptops or iPads etc) to staff at bedtime (9.00pm Sunday to Thursday and 9.15pm Friday and Saturday).

Boarders in Years 10-13 may keep their phones overnight though they are expected only to use them in an emergency.

4.12 Boarding trips are distinct from school trips as they happen during boarders' free time and as such boarders are permitted to take mobile phones. Duty staff carry the Embley Boarding Mobile Phone to enable contact (usually for emergencies) between staff and boarders via call or text message during trips.

4.13 Boarding staff will communicate with parents/guardians where there are concerns over a boarder's use of their mobile phone in their free time.

4.14 Where there are instances of repeated non-compliance boarding staff may decide to confiscate a boarder's phone and this will be discussed with parents/guardian and the boarder may be required to hand in their phone at certain times for a period of time.

5 Email

5.1 E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can nurture significant educational benefits.

5.2 In the school context, e-mail should not be considered private and Embley reserves the right to monitor e-mail. There is a balance to be achieved between necessary monitoring to maintain the safety of staff and pupils and the preservation of human rights, both of which are covered by recent legislation.

5.3 It should be noted that under United Learning regulations, e-mail that has been provided by the school is to be used only for school business and that personal data is not to be stored anywhere on the LAN.

5.4 The following general points should be noted by staff:

- Pupils may only use approved e-mail accounts on the school system and access to external personal email accounts is blocked during the working day.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

  All e-mail content (staff and pupils) is actively monitored by our filtering and safeguarding module within our Securly Filtering Aware solution for the safety of all staff and pupils at the school.

6 Publishing of Pupil Images

6.1 Photographs that include pupils add a liveliness and interest to a website or blog that is difficult to achieve in any other way. Nevertheless, the security of staff and pupils must come first. Sadly, although common in newspapers, the publishing of pupils' full names (including surname) with their photographs is not acceptable. Web images could be misused and individual pupils identified unless broad descriptions are used.

6.2 Photographs of a pupil should not be published without the parent's or carer's written permission. Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

- Pupils' full names (including surname) will not be used anywhere on the website, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

7 Social Networking Access

7.1 Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments. For use by responsible adults, social networking sites provide easy to use, free facilities; although they often feature advertising intrudes and may be dubious in content.

7.2 Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published:

a) Examples include: blogs, wikis, Facebook, X, Snapchat, Instagram, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger, P2P sites and many others.
b) Embley will block/filter access to social networking sites where appropriate both on and offsite on Embley managed devices.
c) Newsgroups will be blocked unless a specific use is approved. In Prep School children have access to First News from Year 3 in order to access the news in an age-appropriate way.
d) Pupils are to be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
e) Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
f) Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for pupils on a personal basis.

g) Where age appropriate, pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
h) Pupils should be advised not to publish specific and detailed private thoughts.
i) The school should be aware that bullying can take place through social networking particularly when a space has been setup without a password and others are invited to see the bully's comments.

7.3 This advice is communicated to pupils through presentations, Safer Internet Day events, the PSHE programme (and additionally in Computer Science lessons in Prep) and through the tutor programme.

7.4 Pupils will be educated regarding risks associated with misinformation, disinformation, conspiracy theories, algorithm-driven content and emerging online platforms.

8 Artificial Intelligence and Emerging Technologies

Embley recognises that Generative AI technologies present both educational opportunities and safeguarding risks. Pupils will be educated about:

- AI-generated misinformation and disinformation.
- Deepfake images, video and audio.
- AI-assisted cyberbullying and harassment.
- The limitations and potential inaccuracies of AI-generated content.
- Appropriate and ethical use of AI tools for learning.

Staff and pupils must not use AI tools to create, share or manipulate content intended to intimidate, harass, deceive or cause harm to another person.

9 E-Safety for Boarders

9.1 All boarding pupils are subject to the Embley E-Safety policy guidelines when using personal or school electronic devices. Pupils in the Boarding House must not:

- Download music/film which breaches copyright laws
- Attempt to access gambling sites
- Attempt to use unauthorised file-sharing sites

9.2 Boarders must accept responsibility for the electronic equipment they bring to school and must ensure it is stored securely (and appropriately insured).

9.3 If the use of mobile devices is abused, sanctions may include confiscation of devices, or additional restrictions on the use of the internet during the evening and the weekend.

9.4 Pupils in the Boarding House remain responsible for their electronic safety when accessing the internet via their own mobile device and must abide by the terms and conditions contained within the E-Safety and Mobile Phone policy and the Acceptable use of ICT and digital resources policy which they have all agreed to and signed.

9.5 All internet activity on a boarder's own device connected to the school's wifi will still be subject to the safeguarding filtering rules the school has in place.

9 Data Protection

Embley recognises cyber security as a safeguarding issue. Staff and pupils are expected to support the security of school systems through appropriate password management, multifactor authentication where provided, and prompt reporting of suspected cyber incidents.

9.1 As part of its everyday activities, United Learning will use or "process" personal data. Details of the type of data we collect and the way it is used can be found in our Privacy Notice (https://www.hampshirecs.org.uk/privacy-policy/)

9.2 The Data Controller for all personal information held by UCST (UCST is registered with the Information Commissioner's Office (ICO). The registration number is Z53307X.

The Data Protection Officer for United Learning is Alison Hussain. They are responsible for ensuring that the Group complies with Data Protection Law. They can be contacted on company.secretary@unitedlearning.org.uk or on 01832 864538.

9.3 Everyone who uses or accesses school systems has a responsibility to protect the data we hold. Pupils should not give access to school systems (by sharing their username or password) and should not transfer data (including photographs) outside of the school network with specific permission to do so.

10 Sites for reference and e-Safety Guidance

Child Exploitation & Online Protection Centre	https://www.ceopeducation.co.uk
UK Safer Internet Centre	http://saferinternet.org.uk
Internet Watch Foundation	http://www.iwf.org.uk
Childnet	http://www.childnet.com
NSPCC	http://www.nspcc.org.uk/
Childline	http://www.childline.org.uk/

11 Relevant Legislation

11.1 **The Computer Misuse Act 1990** - makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data.

The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

11.2 **Public Order Act 1986** – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

11.3 **Communications Act 2003** - There are 2 separate offences under this act of relevance:

- sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
- sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

12 Acceptable Use Policies

All pupils and staff are required to subscribe to the school's Acceptable Use Policies. These policies share core themes outlining the need for responsible and safe use of school computers, iPads and internet access. These AUPs are differentiated for different year groups to enable necessary e-safety education to occur at all stages. Examples of the AUPs follow:

12.1 Acceptable Use policy, **Reception, Year 1 & Year 2**

12.2 Acceptable Use policy, **years 3 to 6:**

EMBLEY
HAMPSHIRE

Introduction

Digital resources in our context refer to school Information and Communications Technology (ICT) systems and equipment (such as desktop computers, laptops, tablets, other mobile devices, printers, scanners, photocopiers and other peripherals), as well as programs, applications and online services available through the school network or the internet.

This policy applies both within school and whenever school digital resources are accessed remotely from any device.

At Embley, digital resources are used to support teaching, learning, creativity, collaboration and communication. We encourage pupils to use technology safely, responsibly and respectfully as part of their education and wider school experience.

By signing this agreement, parents/guardians acknowledge their responsibility to support their child in following the expectations outlined within this policy.

Ethos

1. The school aims to create an environment in which we work collaboratively to encourage academic ambition, belief in oneself and compassion for others, and where all are valued as individuals.
2. The school expects members of the school community to show respect and consideration for themselves and others and to behave compassionately and appropriately.
3. The school will not tolerate any form of bullying, harassment, discrimination or deliberate misuse of digital resources.
4. The school expects pupils to use good judgment and behave in a way that reflects positively on themselves and the school.
5. An authorised representative of the school may view, with just reason and without notice, communications sent or received, material stored on school systems or logs of websites visited. Data stored on school systems remains the property of the school.

Equipment/Hardware

1. Pupils are expected to look after their school iPad and ensure it remains in its protective case.
2. Pupils are responsible for ensuring their iPad is fully charged and ready for school each day.
3. Pupils are not permitted to bring their personal mobile phone into school as per the school's Mobile Phone Policy.
4. Pupils must not damage or interfere with school ICT systems or equipment.
5. Pupils must not install or remove unauthorised software or applications.
6. School printing facilities should only be used for academic work and unnecessary printing should be avoided.
7. Access to school digital resources is a privilege and may be revoked if misused.

8. Mobile Device Management (MDM) software and content filtering software are installed on school devices to support safeguarding and device management.

iPad Care, Insurance and Charges

1. Pupils are expected to take appropriate care of school-issued equipment and help ensure its continued working condition and security.
2. Any damage or malfunction should be reported to the IT Department immediately.
3. Lost, stolen or vandalised devices should be reported to the IT Department as soon as possible.
4. The iPad protective case must not be removed unless authorised by the school or IT Department.
5. Equipment must be returned in full working order upon request or when leaving Embley.
6. Pupils are expected to comply fully with the school's Responsible Use Policy.
7. Unlicensed or harmful software must not be installed on school devices.
8. MDM (Mobile Device Management) software is used to manage school devices.
9. Content filtering software is installed and must not be tampered with or disabled.
10. Accidental damage outside of normal device malfunction (for example smashed screens, bent devices or water damage) will incur a £100 insurance claim charge.
11. Deliberate damage, reckless handling, loss or theft not covered by insurance will incur a replacement charge of £400 including VAT.
12. Upon leaving Embley, failure to return the protective iPad case, or returning a case that has been deliberately damaged or defaced (including graffiti), will incur a replacement charge of £30. Failure to return the charging power block will incur a £15 replacement charge and failure to return the charging cable will incur a £10 replacement charge. For boarding pupils, replacement key fobs will be charged at £10 each, although the initial issue of a key fob is provided at no cost.

Privacy, Data and Security

1. Pupils must keep passwords secure and confidential.
2. Devices connecting to the school network must be protected with a password and/or passcode.
3. Pupils must not use another pupil's username or password.
4. Pupils must respect the privacy of others and must not attempt to access another person's data.
5. Sharing personal information online may be dangerous and unlawful.
6. Pupils must not attempt to bypass school security measures.
7. Devices may be subject to investigation where misuse or safeguarding concerns exist.

Academic Integrity, Plagiarism and Artificial Intelligence Use

1. Plagiarism in any form is unacceptable. This includes direct copying, paraphrasing without citation, submitting another person's work as one's own, or submitting work generated by Artificial Intelligence (AI) without acknowledgement.

2. Microsoft Copilot is currently the only AI platform officially supported and approved for use within United Learning.
3. Any use of other AI platforms or tools must only take place with explicit permission from a member of staff or the school.
4. AI tools should be used to support learning rather than replace original thinking or creativity.
5. Pupils should seek guidance from staff if unsure about the appropriate use of AI or digital resources.

Online Behaviour and Communication

1. Pupils must communicate respectfully and appropriately online.
2. Bullying, harassment or intimidation using digital resources will not be tolerated.
3. Pupils must not access or share inappropriate or illegal material.
4. Any concerning online behaviour should be reported to a member of staff immediately.

Monitoring and Safeguarding

1. The school monitors the use of its digital resources to maintain safeguarding and security. Monitoring may include internet activity, application usage, email usage and network logs.
2. Access to school systems may be restricted or removed where misuse is identified.

Breach of this Policy

Failure to comply with this Responsible Use Policy may result in:

1. Removal of access to digital resources.
2. School disciplinary action.
3. Financial charges for damage or loss.
4. Referral to external agencies where appropriate.

Parent/Guardian Agreement

I have read and understood the Embley Responsible Use Policy and discussed the importance of online safety and responsible digital behaviour with my child.

I understand that the school will take appropriate action if these expectations are not followed, which may include restricted access to digital resources and disciplinary action in line with school policies.

I understand that while Embley takes all reasonable precautions to filter and monitor online content, it cannot guarantee that all inappropriate material can be prevented.

I give permission for my child to use the school's computers, digital resources and internet services in accordance with this policy.

Parent / Guardian Name: _____

Signature: _____

Date: _____

(Please note: Signing this agreement will usually take place through the process provided to parents via Embley's School Portal. Printed copies can be made available where required.)

EMBLEY
HAMPSHIRE

Think then CLICK

I will use my school device **as guided by an adult**

I only use websites for **educational purposes**

I immediately close any webpage I don't like

I will **tell an adult** if I see anything I am unhappy with

I will **never** arrange to meet anyone **I don't know**

I only communicate with **people I know** or an **adult has approved**

I ask permission before opening messages from people I don't know

I communicate online in a **polite and friendly** manner

I keep **passwords, addresses and phone numbers** secret

I will **not harass, annoy or upset others** by my online behaviour

12.5 Acceptable Use Policy for Senior School pupils

Responsible Use of Information and Communications Technology & Resources

Introduction

Digital resources in our context refer to school Information and Communications Technology (ICT) systems and equipment (such as desktop computers, laptops, tablets, other mobile devices, printers, scanners, photocopiers and other peripherals), as well as programs, applications and online services available through the school network or the internet.

This policy applies both within school and whenever school digital resources are accessed remotely from any device.

At Embley, digital resources are used to support teaching, learning, creativity, collaboration and communication. We encourage pupils to use technology safely, responsibly and respectfully as part of their education and wider school experience.

By signing this agreement, parents/guardians acknowledge their responsibility to support their child in following the expectations outlined within this policy.

Ethos

6. The school aims to create an environment in which we work collaboratively to encourage academic ambition, belief in oneself and compassion for others, and where all are valued as individuals.
7. The school expects members of the school community to show respect and consideration for themselves and others and to behave compassionately and appropriately.
8. The school will not tolerate any form of bullying, harassment, discrimination or deliberate misuse of digital resources.
9. The school expects pupils to use good judgment and behave in a way that reflects positively on themselves and the school.
10. An authorised representative of the school may view, with just reason and without notice, communications sent or received, material stored on school systems or logs of websites visited. Data stored on school systems remains the property of the school.

Equipment / Hardware

1. I will look after my school iPad and ensure it remains in its protective case.
2. I understand that I am responsible for ensuring my iPad is fully charged and ready for school every day.
3. I understand that I am solely responsible for any personal devices brought into school.
4. I will not damage or interfere with school ICT systems or equipment.
5. I will not install or remove unauthorised software or applications.
6. I will only use printing facilities for academic work and avoid unnecessary printing.
7. I understand that the use of school digital resources is a privilege and may be revoked if misused.

8. I understand that Mobile Device Management (MDM) software and content filtering software are installed on school devices.

iPad care, insurance and charges

1. I will take the necessary precautions to ensure the continued working condition and security of the equipment.
2. In the event of damage or malfunction, I will report this to the IT Department immediately.
3. If the equipment is lost, stolen or vandalised, I will notify the IT Department as soon as possible.
4. The iPad protective case must not be removed unless authorised by the school or IT Department.
5. I agree to return the equipment in full working order upon request or when leaving Embley.
6. I agree to comply fully with the school's Responsible Use Policy.
7. I understand that unlicensed or harmful software must not be installed on the device.
8. I understand that MDM (Mobile Device Management) software is used to manage my device.
9. I understand that content filtering software is installed and must not be tampered with.
10. Accidental damage outside of device malfunction (e.g. smashed screen, bent device or water damage) will incur a £100 insurance claim charge.
11. Deliberate damage, reckless handling, loss or theft not covered by insurance will incur a replacement charge of £400 including VAT.
12. Upon leaving Embley, failure to return the protective iPad case, or returning a case that has been deliberately damaged or defaced (including graffiti), will incur a replacement charge of £30. Failure to return the charging power block will incur a £15 replacement charge and failure to return the charging cable will incur a £10 replacement charge. For boarding pupils, replacement key fobs will be charged at £10 each, although the initial issue of a key fob is provided at no additional cost.

Privacy, Data & Security

1. I will keep my passwords secure and confidential.
2. Devices connecting to the school network must be protected with a password and/or passcode.
3. I will not use another pupil's username or password.
4. I will respect the privacy of others and not attempt to access their data.
5. I understand that sharing personal information online may be dangerous and unlawful.
6. I will not attempt to bypass school security measures.
7. I understand that devices may be subject to investigation where misuse or safeguarding concerns exist.

Academic integrity, Plagiarism and Artificial Intelligence use

1. I understand that plagiarism in any form is unacceptable.

2. This includes direct copying, paraphrasing without citation, submitting another person's work as my own, or submitting work generated by Artificial Intelligence (AI) without acknowledgement.
3. I understand that Microsoft Copilot is currently the only AI platform officially supported and approved for use within United Learning, Embley's parent company.
4. Any use of other AI platforms or tools must only take place with explicit permission from a member of staff or the school.
5. I will use AI tools to support learning rather than replace my own thinking or originality.
6. I will seek guidance from staff if unsure about the appropriate use of AI or digital resources.

Online behavior and communication

1. I will communicate respectfully and appropriately online.
2. I will not bully, harass or intimidate others using digital resources.
3. I will not access or share inappropriate or illegal material.
4. I will report concerning online behaviour to a member of staff immediately.

Monitor and Safeguarding

1. I understand that the school monitors the use of its digital resources to maintain safeguarding and security.
2. Monitoring may include internet activity, application usage, email usage and network logs.
3. Access to school systems may be restricted or removed where misuse is identified.

Breach of this policy

Failure to comply with this Responsible Use Policy may result in:

1. Removal of access to digital resources.
2. School disciplinary action.
3. Financial charges for damage or loss.
4. Referral to external agencies where appropriate.

Parental Agreement

I have read and understood the Embley Responsible Use Policy and discussed the importance of online safety and responsible digital behaviour with my child.

I understand that the school will take appropriate action if these expectations are not followed, which may include restricted access to digital resources and disciplinary action in line with school policies.

I understand that while Embley takes all reasonable precautions to filter and monitor online content, it cannot guarantee that all inappropriate material can be prevented.

I give permission for my child to use the school's computers, digital resources and internet services in accordance with this policy.

Parent / Guardian Name: _____

Signature: _____

Date: _____

(Please note: Signing this agreement will usually take place through the process provided to parents via Embley's School Portal. Printed copies can be made available where required.)

Student Agreement

I have read and understood the Embley Responsible Use Policy and agree to use the school's digital resources responsibly, safely and respectfully. I understand that access to school ICT systems, devices and internet services is a privilege and that misuse may result in restrictions, disciplinary action or financial charges where appropriate. I also understand the importance of online safety, academic integrity and the responsible use of AI tools.

Student Name: _____

Signature: _____

Date: _____

(Please note: Signing this agreement will usually take place through the process provided to students via Embley's School Portal before joining and upon collection of their Embley iPad. Printed copies can be made available where required.)

12.5 Acceptable Use Policy for staff

1 Policy statement

1.1 Embley (EMBLEY) provide computers for staff use; access to the internet provides vast, diverse, and unique digital resources. Our goal in providing this access is to promote educational excellence by facilitating resource sharing, innovation and communication.

1.2 Digital resources in our context refer to school Information and Communications Technology systems and equipment (such as desktop computers, laptops, tablets and other mobile devices, printers, scanners, photocopiers and other peripherals), but also to programs, applications and services available on the network or on the Internet. Therefore, we expect that this agreement is adhered to both in School and when our digital resources are accessed remotely.

1.3 Teachers, support staff, students and members of the wider school community at Embley are encouraged to use our digital resources as a way to create and share content and resources, as well

as a means to connect with others and network within and outside the school community, always with the overarching aim of supporting and enhancing teaching and learning.

1.4 Tablets and computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and to help to ensure they remain available to all.

1.5 Staff should also read this policy in conjunction with the Staff-Student Relationship Letter, which is received annually, and United Learning disciplinary procedures document, which is available on the United Learning Hub.

2 Ethos

2.1 The school aims to create an environment in which we work collaboratively to encourage ambition, belief in oneself and compassion for others, and where all are valued as individuals; underpinned by a culture of respect for ourselves and others. The school therefore expects that its digital resources are used in this spirit.

2.2 The School expects the members of the School Community to show respect and consideration for self and others and to behave kindly and appropriately, and in such a way that would not disrupt the use of our digital resources.

2.3 The School will not tolerate any form of bullying or deliberate misuse.

2.4 The School expects the members of the school community to use good judgement and behave in such a way that will reflect well on them and the School.

3 Internet

3.1 Access to the Internet at Embley is provided primarily for educational and school-related activities. This applies to both staff and students; however, distinctions apply based on age group:

- Prep School pupils must continue to use the Internet solely for educational purposes unless otherwise authorised by a member of staff.
- Senior School students are permitted to access the Internet for personal use after the school day, provided their usage remains appropriate and in line with school guidelines.

Securly Web Filtering remains active at all times across the school network. It will continue to monitor online activity and restrict access to inappropriate websites, regardless of the time of day or device used.

Although certain social media restrictions are lifted for boarding students outside of core school hours, Embley reserves the right to reinstate these restrictions at any time if usage is deemed inappropriate or excessive.

Please note that privacy is not guaranteed. The school may monitor and access any personal data created or accessed via email, the internet, or school-provided devices and software, without prior notice or the user's permission. This monitoring is in place to ensure safeguarding, network security, and appropriate use of school systems.

3.2 Staff should not issue the school web address to any site that is filtered and therefore is intentionally inaccessible from the school network (e.g. some social networking sites). Staff should also not issue their work e-mail addresses to any companies that may generate excessive junk mail.

3.3 Users shall not visit, download from, upload to or otherwise access websites or other electronic media displaying or promoting pornography, child sex abuse images, racial or religious hate, illegal activity or other potentially offensive material.

3.4 Deliberate access to websites or other electronic media containing child sex abuse images, material in contravention of the Obscene Publications Act 1959 and 1964 or material inciting racial hatred will be reported to the police.

3.5 Users shall not use Embley resources for running a private business.

3.6 Users shall not visit or post to websites or other electronic media that may be defamatory to the school or bring the school into disrepute. Defamation of the school would be seen as a breach of an employee's contract of employment.

3.7 Users shall not visit, upload or download from websites or other electronic media which may cause the user or school to contravene the Copyright, Designs and Patent Act 1988. Refer to section d) below on Copyright.

3.8 Users shall not access, process or share data in a manner that breaches the UK General Data Protection Regulation (UK GDPR) or the Data Protection Act 2018.

3.9 Users shall not attempt to interfere with the normal operation of the school's ICT resources by propagating or attempting to propagate viruses, spyware, malware or other malicious code.

3.10 Users must obtain prior approval at Senior Leadership level to set-up internet sites on school computer facilities, publish pages on external internet sites containing information relating to the school, enter into agreements on behalf of themselves or the school via a network or electronic system, transmit unsolicited commercial or advertising material to other users of a network or to other organisations and use school computing facilities for external gain.

3.12 Users will inform the Designated Safeguarding Lead and the Head of I.T if they accidentally encounter inappropriate material whilst using the School's digital resources.

3.13 Embley will routinely monitor and audit the use of the internet to ensure compliance.

3.12 On evidence provided, a user may be disciplined by the school. At the same time, if a user behaves in an unlawful way, the user's behaviour may be reported to the police.

4 Email

4.1 Work or activity conducted through email must be directly related to your school work.

4.2 Staff must not give their password or login name to anyone at any time.

4.3 Users shall not download, use or upload or send by email any material which in doing so infringes copyright and they must not view, upload or download or send by email any material which is likely to be unsuitable for children or schools. This applies to material of a violent, dangerous, racist or inappropriate sexual content. If you are unsure about this, or any materials, you must ask your line manager.

4.4 Be polite and appreciate that other users might have different views from your own. The use of strong language, abusive language (swearing) or aggressive behaviour is not allowed. You should not

write anything on a website or send by email anything which could be offensive. If you receive an email containing any of the above always report such messages to a member of the IT support team.

4.5 Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

4.6 Embley may monitor without notice external and internal email and has the right, if it wishes, to have access to read any matter sent or received by the user.

5 Use of Social Media, Internet Messaging and Chat Rooms

5.1 Whilst the school appreciates that networking software such as Facebook, Instagram or X provide opportunities for personal expression, the creation of communities, collaboration and sharing, the use of social media, internet messaging and chat rooms must be used with caution and in accordance with our social media policy.

5.2 EMBLEY tablets and computers are used for educational purposes or in the administration of the school. During school hours, access to activities such as gaming, shopping and social media will be blocked.

5.3 Staff must not communicate directly with students using social media, internet messaging and chat rooms.

5.4 Always be wary about revealing any of your own personal information or school information online.

EMBLEY may monitor without notice any posts, blogs and other forms of messaging and has the right, if it wishes, to have access to read any matter sent or received by the user.

6 Copyright

6.1 Users must abide by copyright legislation if the intention is to use or publish materials through the internet. The use of online materials for teaching and learning is different from the use of printed and television or audio broadcast materials, which are covered by the Copyright Licensing Agency (CLA) and the Educational Recording Agency (ERA).

6.2 All materials published on the web (irrespective of format) are subject to copyright law and may not be copied or otherwise reproduced without the copyright owner's permission. Permission may be granted by the owner as stated at their site, or it may need to be obtained directly from the owner. It is insufficient just to acknowledge the source. If Internet materials are clearly labelled as being copyright-free or in the public domain then it may be legally acceptable to use the materials.

6.3 Similar care must be used in copying music, video or music from CDs, CDROMs or DVDs. Possession of the originals does not automatically entitle the user to copy the contents in any format, and it may be illegal unless expressly authorised on the media or packaging itself.

6.4 Further information on copyright issues may be found in the UCST and ULT policy on Copyright.

7 Use of Personal Laptops on the School Network

7.1 Physical wired connections for personal laptops or mobile computing devices to the network is not permitted. However, you can connect your personal devices to the internet via the school wi-fi

providing you have read and completed the BYOD form. If you choose to do so, the filtering policy will apply to those devices.

7.2 The use of the camera function on any personal mobile device is strictly forbidden at all times. Photographs may only be taken using a school tablet and for marketing or educational purposes, and always with the consent of those being photographed.

7.3 If you bring a personal laptop or other personal computing devices (such as tablets or smartphones) into school, they are entirely your responsibility. If you access the internet whilst in school, it is expected that you will abide by the ethos of this document.

8 Use of Personal Storage Items

8.1 Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.

8.2 Any mobile storage devices such as USB drives or external hard drives are restricted from being used at the school in line with the UL policy.

8.3 The need for personal storage devices is eliminated by the appropriate use of OneDrive, which the school provides and expects users to utilise appropriate and effectively.

9 Data Security (including guidelines on creation and security of passwords)

9.1 Under no circumstances should personal or other confidential information held on computer be disclosed to unauthorised persons.

9.2 The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computer Misuse Act 1990.

9.3 Protect yourself by keeping your password private; never use someone else's username and password, even if they ask you to do it.

9.4 Passwords must comply with United Learning technical standards and should be strong, unique and not shared with anyone else. Multifactor authentication must be used where provided.

9.5 Confidential or sensitive corporate data is not to be taken off-site. (See 8.3)

9.6 Be wary of revealing any of your own personal information or school information online.

9.7 Respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk and would be classed as a direct breach of this policy.

9.8 Your data is your responsibility. Embley network may review your files and communications to ensure that you are using the system responsibly.

10 Health and Safety

10.1 Protect ICT equipment from spillages by not eating or drinking around it.

10.2 In addition, please read this document in conjunction with the school's Health and Safety Policy document.

11 Equipment

11.1 Installing or attempting to install or storing unauthorised programs of any type anywhere on the network is not permitted.

11.2 Do not damage or disable ICT equipment or intentionally waste ICT resources. This puts your work at risk and reduces the availability of ICT equipment for everyone.

11.3 Embley students are encouraged to use digital resources where possible. If printing is required, this will need to be sent to your teacher for approval and action. Art Students will have the ability to print in this area and this usage will be recorded.

11.4 You will look after your school issued tablet and ensure it is always kept in its case.

12 Monitoring by the School

12.1 Staff must only access those services they have been given permission to use, and they must not access the internet or email for inappropriate purposes.

12.2 Embley will routinely monitor and audit the use of the internet to ensure compliance with the above policy.

13 Sanctions for Misuse

13.1 As previously stated, on evidence provided, a user may be disciplined by the school. If the above policy is violated, access to network will be withdrawn and you will be subjected to disciplinary action.

13.2 The school reserves the right to discipline any member of staff for actions taken outside of school if they are intended to have an effect on a staff member or they adversely affect the safety and well-being of student and staff members while in school.

13.3 The user's behaviour may be reported to the police.

13.4 If an employee has their network access withdrawn, with or without notice, and wishes to appeal against the decision, this should be done via the grievance procedure as outlined in the staff handbook.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Signature: .....

Name: .....

Date: .....

12.6 EMBLEY Prep School Mobile Phone Policy for Years 3 to 6

Pupils at Embley Prep are not allowed to have or use mobile phones at any point during the school day. Parents are reminded that in cases of emergency, the Prep School Office remains the main point of contact.

Any pupil who brings a mobile phone into school must hand it into the Prep School office at the beginning of the school day and collect it at the end of the school day. The phone must be clearly named.

I confirm that my son/daughter will always follow the school's mobile phone policy.

I am aware that the School will not take any responsibility for any loss, damage or misuse of pupils' mobile phones or any other personal electronic devices.

The use of any camera function on mobile phones while pupils are under staff supervision (including on the bus) is strictly forbidden.

NAME OF PUPIL: ---------- FORM: .....

MOBILE PHONE NO: .....

MAKE/MODEL: ----------
SERIAL NO: .....

DESCRIPTION: .....

SIGNATURE OF PARENT/GUARDIAN: ----------

DATE: ----------

13 Document Information

Version Number	8.4
Reason for Version Change	Update of mobile phone policy
Name of owner/author	Leah Goodey
Name of individual/department responsible	Leah Goodey, Deputy Head Rob Clare, Director of Studies Lesley Johnson, Head of Computing and ICT Luke Adams, Head of I.T Lisa Johnson, Data Manager & Data Protection Lead
United Learning Independent Schools/Academies/Both	United Learning Independent Schools
Target Audience	Public
Date Authorised	2 June 2026
Date issued	2 June 2026
Where available	United Learning Hub, Network, school website
Review Date	August 2027 or as events and legislation require